Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 01 July 2005

Current Nationwide Threat Level is
ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports that U.S. Border Patrol agents have been operating near Santa Fe and elsewhere in northern New Mexico this week to gauge the extent of human smuggling in areas farther from the Mexican border. (See item 11)
- The Business Journal of Phoenix reports that a statewide database designed to give the public instant access to health, human services and emergency response information made its debut in Arizona Wednesday. (See item 26)

Energy Sector

Current Electricity Sector Threat Alert Levels:
[set manually]

1. *June 30, Federal Energy Regulatory Commission* — **Governments and agencies cooperate to ensure electric reliability in North America.** A bilateral working group from the United States and Canada will address key issues related to electricity reliability in North America. The terms of reference for the Bilateral Electric Reliability Oversight Group were announced on Thursday, June 30, by Samuel W. Bodman, U.S. Secretary of Energy; Pat Wood, III, Chairman of the Federal Energy Regulatory Commission (FERC); the Honorable R. John Efford, Minister of Natural Resources Canada; and Dwight Duncan, Ontario Minister of Energy. The Bilateral Group will consult on the establishment of an international framework for reliability and issues related to international aspects of mandatory reliability standards in North America. It commits

to developing principles to guide the establishment of a reliability organization that can function on an international basis; coordinating on the electric reliability standards process; and consulting on policy and regulatory issues surrounding reliability. The Bilateral Group is comprised of representatives from the U.S. Department of Energy, FERC and the Federal−Provincial−Territorial Electricity Working Group of the Canadian Council of Energy Ministers, with assistance from the Department of Foreign Affairs and International Trade and the U.S. Department of State.
Source: http://www.ferc.gov/press−room/pr−current/06−30−05−reliabili ty.asp

2. *June 29, ABC7Chicago.com* — **Utility urged to link alarm system to emergency center.** The city of Chicago is pushing utility ComEd to link its monitoring and alarm systems with the city's 911 Center. This is in response to a fire on Friday, June 24, at a substation that left thousands without power for hours. ComEd determined the fire at the substation on West Cermak was the result of an underground transmission cable failure. City officials say linking ComEd's alarm system to the 911 Center would allow Chicago emergency crews to be better prepared because they'll be notified about a problem at the same time ComEd is notified.
Source: http://abclocal.go.com/wls/news/062905_ns_comed.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

3. *June 30, New York Times* — **Bank of America to buy MBNA.** The Bank of America Corporation said on Thursday, June 30, that it would acquire the MBNA Corporation, a leading issuer of credit cards, in a deal valued at $35 billion in stock and cash. The acquisition would make Bank of America the largest credit card issuer in the United States, with the combination giving the financial services giant a 20 percent market share in an industry rapidly consolidating. For MBNA, which has relied on its partnerships with such affinity groups as college alumni and professional association for much of its growth, the merger would give it access to Bank of America's large network of retail bank branches stores to attract new customers. Bank of America, meanwhile, gains access to MBNA's marketing expertise along with credit card portfolio that is made up of the lowest−risk borrowers in the industry. The deal is expected to close in the fourth quarter of 2005.
Source: http://www.nytimes.com/2005/06/30/business/30cnd−america.htm l?hp&ex=1120190400&en=fb2fa8561e8fa776&ei=5094&partner=homep age

4. *June 30, CBS MarketWatch* — **Regulators issue manual to curb money laundering.** In an effort to consistently apply standards to fight money laundering and the use of banks for illicit purposes, a group of U.S. financial regulators on Thursday, June 30, issued a new manual about examining banks. The Federal Financial Institutions Examination Council Bank Secrecy Act/Anti−Money Laundering (FFIEC BSA/AML) gives regulators guidelines for measuring a bank's compliance with a U.S. law that requires reports about suspicious activities by customers. The banking industry had sought a single set of rules to turn to with questions about money laundering and suspicious activity at banks. Federal banking agencies will begin using the manual in the third quarter of 2005. FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision and to make recommendations to promote uniformity in the supervision of financial institutions.
FFIEC BSA/AML Examination Manual: http://www.ffiec.gov/press/pr063005.htm
Source: http://www.marketwatch.com/news/story.asp?guid=%7BF3EAF6D1−482F−4F2D−A719−E0967B640F08%7D&siteid=google

5. *June 30, Government Accountability Office* — **GAO−05−710: Identity Theft: Some Outreach Efforts to Promote Awareness of New Consumer Rights Are Under Way (Report).** The Fair and Accurate Credit Transactions (FACT) Act of 2003 which amended the Fair Credit Reporting Act (FCRA), contains provisions intended to help consumers remedy the effects of identity theft. For example, section 609(e) of the amended FCRA gives identity theft victims the right to obtain records of fraudulent business transactions, and section 609(d) requires the Federal Trade Commission (FTC) to develop a model summary of identity theft victims' rights. This report provides information on (1) outreach efforts to inform consumers, businesses, and law enforcement entities about section 609(e); (2) the views of relevant groups on the provision's expected impact; and (3) FTC's process for developing its model summary of rights and views on the summary's potential usefulness.
Highlights: http://www.gao.gov/highlights/d05710high.pdf
Source: http://www.gao.gov/new.items/d05710.pdf

6. *June 30, Department of the Treasury* — **Treasury designation targets individuals leading Syria's military presence in Lebanon.** The U.S. Department of the Treasury on Thursday, June 30, named Ghazi Kanaan and Rustum Ghazali Specially Designated Nationals (SDNs) of Syria pursuant to Executive Order 13338, which is aimed at financially isolating individuals and entities contributing to the Government of Syria's problematic behavior. "Actions like today's are intended to financially isolate bad actors supporting Syria's efforts to destabilize its neighbors," said Treasury Secretary John W. Snow. Information available to the U.S. Government indicates that Kanaan and Ghazali have directed the Syrian Arab Republic Government's (SARG) military and security presence in Lebanon and/or contributed to the SARG's support for terrorism. Both Ghazali and Kanaan allegedly engaged in a variety of corrupt activities and were reportedly the beneficiaries of corrupt business deals during their respective tenures in Lebanon. Thursday's designation freezes any assets the designees may have located in the United States, and prohibits U.S. persons from engaging in transactions with these individuals.
Source: http://www.treasury.gov/press/releases/js2617.htm

7. *June 30, Reuters* — **Terror insurance needs change if extended.** A program of U.S. government guarantees to cover high−priced terrorism insurance served its purpose after the September 11, 2001 attacks, but should not be extended in its current form, the Department of Treasury said in a report issued on Thursday, June 30. The Treasury said extending the Terrorism Risk Insurance Act, or TRIA, in its current form would hinder the further development of the insurance market by crowding out innovation. The Bush administration would only support extending TRIA beyond its December 31 expiration, it said, if changes were made to the law to boost the event size that triggers coverage, increase deductibles and co−payments and eliminate some lines of insurance from the program. Treasury's findings are expected to drive debate in Congress on whether to extend TRIA. The law, enacted after the September 11 attacks, created a temporary federal program of shared compensation for losses from terrorist events. It was seen as critical to sustaining construction and the economy at a time when insurers were reluctant to offer coverage.
Treasury report: http://www.treasury.gov/press/releases/reports/063005%20tria %20study.pdf
Source: http://news.yahoo.com/news?tmpl=story&u=/nm/20050630/pl_nm/financial_terrorism_dc_1

[Return to top]

Transportation and Border Security Sector

8. *June 30, Washington Post* — **Stray plane sets off evacuation of Capitol.** The U.S. Capitol was evacuated on Wednesday evening, June 29, after a small plane flying at a rapid clip entered Washington, DC's restricted airspace and prompted a scramble by federal officials to launch fighter jets and other aircraft to intercept the plane. The urgency of the evacuation order diminished after about two minutes as the pilot of the twin−engine turboprob aircraft responded quickly to the interception and changed course, federal officials said. Still, the intrusion−−the second in about six weeks in which a small plane violated the airspace−−disrupted a Senate vote and prompted authorities at the White House to move President Bush to a more secure location. The pilot responded "very quickly," said Mike Kucharek, spokesperson for the North American Aerospace Defense Command. In that respect, this incident differed from the May 11 incident, in which the pilot of a Cessna initially failed to respond to flares launched by fighter jets or hand signals from Black Hawk helicopter crews. The Secret Service said the pilot was released after questioning. A Federal Aviation Administration spokesperson said the matter is under investigation.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06/29/AR2005062902957.html?sub=AR

9. *June 30, Department of Transportation* — **Federal Railroad Administration to require stronger "black boxes" for train accident investigations.** Train "black box" data and information will be better safeguarded for use in accident investigations as a result of a Federal Railroad Administration (FRA) final rule requiring improvements in the crash survivability of locomotive event recorders. Under the rule, event recorders will be hardened to prevent the loss of data from exposure to fire, impact shock, fluid immersion, and other potential damage resulting from train accidents. New data required to be captured includes horn activation, cruise control functions and train control operating directives sent to the engineer's onboard display.

Currently, locomotive event recorders capture such information as train speed, use of automatic air brakes, throttle position and cab signal indications. “We are making sure that investigators have more and better information available when working to find the cause of an accident,” said FRA Administrator Joseph H. Boardman. The rule gives railroads four years to replace older−style event recorders that use magnetic tape to store data with new electronic memory modules. The rule also requires railroads to improve inspection, testing and maintenance procedures.
The final rule is available on the FRA’s Website at http://www.fra.dot.gov and in docket number FRA−2003−16357 at http://dms.dot.gov.
Source: http://www.dot.gov/affairs/fra1505.htm

10. *June 30, Christian Science Monitor* — **U.S. tries to stamp 'secure' on passports.** A U.S. passport is the gold standard for travelers as well as terrorists and international criminals. Almost four years after the September 11 terrorist attacks, a government investigation found that it's still possible for individuals on the terrorist watch list as well as wanted criminals to obtain a U.S. passport. That's prompted a new urgency on Capitol Hill to improve security and fraud detection at the State Department, as well as communications with the FBI and the Department of Homeland Security, which maintains a consolidated terrorist watch list. At the same time, controversy continues over the best way to create "fraud proof" passports using new technology like biometric identifiers −− iris scans or fingerprints −− embedded in computer chips within the passport. In 2004, the State Department issued 8.8 million passports from 7,000 locations. During that same year, the State Department's Bureau of Diplomatic Security arrested 500 people for passport fraud, according to the Government Accountability Office, which conducted the investigation. Experts in passport fraud say that significantly more passports are fraudulently obtained every year, in part because it's so easy to buy the documents needed to get a passport. A few hundred or a few thousand dollars can buy a birth certificate in most cities.
Source: http://www.csmonitor.com/2005/0630/p03s01−uspo.html

11. *June 30, Associated Press* — **Border Patrol traffic stops near Santa Fe.** U.S. Border Patrol agents have been operating near Santa Fe and elsewhere in northern New Mexico this week to gauge the extent of human smuggling in areas farther from the Mexican border, Border Patrol spokesperson Doug Mosier said. Illegal immigrant−rights advocates, however, said the patrols are causing worry among Santa Fe−area immigrants. Mosier said the federal agency began an "enforcement action" based out of Albuquerque earlier this week, but he refused to supply details of the operation. Mosier said agents were looking for anything that falls "under the umbrella of homeland security," which could include human, drug or weapons smuggling. The operation is part of a nationwide effort, he said, and is unrelated to any terrorist threat or Independence Day.
Source: http://kvoa.com/Global/story.asp?S=3541523

[Return to top]

Postal and Shipping Sector

12. *June 30, WSTM (NY)* — **Postal Service holds biohazard drills.** The U.S Postal Service has spent several months preparing for a drill to be held Thursday, June 30, at the downtown

Binghamton, NY, mail handling site. Spokesperson Maureen Marion says workers will be evacuated during the exercise. Marion says the drill scenario will involve the discovery of a suspicious letter. Marion says the exercise is similar to one conducted earlier this month at a Rochester, NY, mail handling facility. Another drill is set for next month in Syracuse, NY.
Source: http://www.wstm.com/Global/story.asp?S=3535808

[Return to top]

Agriculture Sector

13. *June 30, Brownfield Network* — **Soybean rust confirmed in new state.** Asian soybean rust has been confirmed in Baldwin County, AL, according to the U.S. Department of Agriculture. Experts from Auburn University in Alabama have been utilizing special traps to monitor spores in the atmosphere. According to Ed Sikora, with Auburn University Extension, the soybeans at sentinel plots in the Baldwin County area are now in the reproductive growth stages. He has indicated that kudzu is widespread throughout Alabama and growing as well. Plant experts have speculated that recent weather conditions may have been favorable for soybean rust spores to move north, out of regions in Florida and Georgia where it has previously been confirmed. Baldwin County borders Florida's western panhandle.
Source: http://www.brownfieldnetwork.com/gestalt/go.cfm?objectid=CDE2A911−C1EC−96BE−15A42F664482C5FF

14. *June 29, Animal and Plant Health Inspection Service* — **Epidemiological investigation into recently confirmed mad cow case.** DNA test results have confirmed that the U.S. Department of Agriculture (USDA) has identified the source herd of the animal determined last week to be positive for mad cow disease −− also known as bovine spongiform encephalopathy (BSE). Based on information the USDA received from the owner, the cow was born and raised in a herd in Texas and was approximately 12 years old. It was sent to a 3D/4D pet food plant in Texas and was selected for sampling on arrival. “The source herd is now under a hold order as we identify animals of interest within the herd. Animals of interest would include any other animals that were born the same year as this animal, as well as any born the year before and the year after. If the age of the animal cannot be pinpointed, then we may expand our inquiry to include all animals in this herd before the feed ban went into place in 1997. We are also interested in any of this animal’s offspring that were born within the last two years. Experience worldwide has shown us that it is highly unusual to find BSE in more than one animal in a herd or in an affected animal’s offspring. Nevertheless, all animals of interest will be tested for BSE," said John Clifford, USDA chief veterinarian.
Source: http://www.aphis.usda.gov/lpa/news/2005/06/jun.html

[Return to top]

Food Sector

15. *June 30, Guardian (United Kingdom)* — **One in six countries facing food shortage.** One in six countries in the world face food shortages this year because of severe droughts that could become semi−permanent, United Nations (UN) scientists warned Wednesday, June 29. Wulf

Killman, chairman of the UN Food and Agriculture Organization's (FAO) climate change group, said the droughts that have devastated crops across Africa, central America, and south−east Asia in the past year are part of an emerging pattern. The FAO and the U.S. government, both of which monitor global food shortages, agree that 34 countries are now experiencing droughts and food shortages and others could join them. Up to 30 million people will need assistance because of the droughts and other natural disasters such as the Asian tsunami. The worst affected countries include Ethiopia, Zimbabwe, Malawi, Eritrea and Zambia, a group of countries where at least 15 million people will go hungry without aid. The situation in Niger, Djibouti and Sudan is reported to be deteriorating rapidly. Many countries have had their worst harvests in more than 10 years and are experiencing their third or fourth severe drought in a few years, the UN said.
Source: http://www.guardian.co.uk/international/story/0,,1517746,00. html

16. *June 30, Associated Press* — **Jamaica will import U.S. beef despite mad cow case.** Jamaica will continue importing beef from the U.S., despite the confirmation there of a case of mad cow disease, an official said. The U.S. Department of Agriculture (USDA) on Friday, June 24, confirmed the disease had been found in an animal that had been born before the U.S. and Canada banned cattle parts in cattle feed, which is how the disease is believed to have spread. Jamaican Agriculture Minister Roger Clarke said there were no scientific grounds to impose a ban. Jamaica does not allow imports of every cut of beef. There is a standing ban on imports of beef intestines, brains, and spinal column byproducts −− the parts most affected by mad cow disease.
Source: http://www.chinapost.com.tw/business/detail.asp?GRP=E&id=645 96

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

17. *June 30, Agence France Presse* — **Portugal orders medicine to counter threat of bird flu pandemic.** Portugal has ordered 2.5 million doses of medication to treat bird flu, enough for a quarter of its population, to prepare for a possible global epidemic of the lethal disease. Francisco Jorge, the deputy director−general for health, said the shipment of Tamiflu, the drug considered the best defense against bird flu for which there is no vaccine, will be delivered in about a year's time. He told state radio RDP it would take Swiss pharmaceuticals giant Roche, the sole manufacturer of the drug, that much time to fulfill the order because it has so far received requests from 25 other nations for the medication. The increasing number of deaths from the lethal H5N1 strain of the avian influenza has raised concerns among health experts that the virus may mutate to a form easily transmitted between humans, possibly sparking a flu pandemic that could kill millions. As a result, the World Health Organization (WHO) has urged governments not to leave plans for how to cope with a pandemic until it is too late.
Source: http://news.yahoo.com/news?tmpl=story&u=/afp/20050630/hl_afp

/healthfluportugal_050630125000

18. *June 30, Fuardian Wandsworth (UK)* — **Methicillin Resistant Staphylococcus Aureus cases fall at London hospital.** Methicillin Resistant Staphylococcus Aureus (MRSA) infections at St. George's Hospital in London, England, have fallen by a third, according to new figures published by the Department of Health. There were 63 bloodstream infections of the antibiotic−resistant bacteria MRSA between April 2004 and March 2005, compared with 93 cases in 2003 to 2004. St. George's Hospital has introduced a range of measures to stop patients acquiring MRSA and other infections while in hospital. Patients are screened for MRSA on admission from other hospitals and nursing homes. A trust−wide campaign continues to encourage doctors and nurses to clean their hands more often with an alcohol disinfectant gel. The hospital has also established a team of specialist nurses to supervise the safe placing of intravenous lines, which are a known source of infection. More recently, St. George's appointed a pharmacist to regulate the prescribing of antibiotics to slow the development of drug−resistant organisms.
Source: http://www.wandsworthguardian.co.uk/display.var.610320.0.mrsa_cases_fall_at_st_georgersquos.php

19. *June 30, North Jersey.com* — **Flu drug fight comes as influenza pandemic fears rise.** A clash between Roche and its biotech partner over the flu−fighting drug, Tamiflu, has erupted into public view amid preparations for an influenza pandemic. Gilead Sciences Inc., one of the largest biotech companies, announced last week it notified Roche it was seeking to terminate their licensing agreement and gain back all the rights to Tamiflu. Roche, a Swiss drug giant whose U.S. pharmaceutical operations are based in Nutley, NJ has been in charge of marketing Tamiflu worldwide and manufacturing it. Gilead claimed Roche failed on both fronts. The biotech company also said Roche shortchanged it by $18 million in royalty payments. Roche said it disagreed with Gilead's position, and defended its investment in Tamiflu. The dispute comes as experts view Tamiflu as a weapon against avian flu, for which there is no vaccine. Jeffrey Levi, senior policy adviser for the Trust for America's Health, said the principal concern is that the Roche−Gilead conflict will lead to reduced production of Tamiflu, which already is in short supply. Roche said it was committed to ensuring the matter did not disrupt production or impinge on supply commitments.
Source: http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFlZUVFeXkyOCZmZ2JlbDdmN3ZxZWVFRXl5NjcxNDcyNSZ5cmlyeTdmNzE3Zjd2cWVlRUV5eTI=

20. *June 30, Denver Post (CO)* — **Colorado reports its first two West Nile cases of the season.** The first two people to contract the West Nile virus in Colorado this year are a 50 year old Weld County woman and a 17 year old Fort Collins male, according to officials. Both cases were confirmed Wednesday, June 29. The Weld County woman developed West Nile virus fever on May 24 but was not hospitalized. The 17−year−old became ill on June 5 and was hospitalized briefly. West Nile is carried by birds and transmitted by mosquitoes that bite the birds. Regularly using repellent containing DEET is the most effective way to avoid mosquito bites, said Douglas Benevento, health department executive director. Colorado is the third state to report human cases of West Nile this year. Two cases were reported earlier this month in Kansas, and three cases were recently reported in South Dakota. A total of 291 human cases of West Nile, including four deaths, was reported in Colorado in 2004. The first full season of

West Nile in Colorado, in 2003, saw 2,947 confirmed cases and 63 deaths.
Source: http://www.denverpost.com/news/ci_2831803

21. *June 29, Reuters* — **Vietnam bird flu toll rises to 39.** A 73−year−old Vietnamese has died from bird flu, taking the country's toll to 39, 19 of them since the virus returned in December, state−run media reported on Thursday. The Hanoi resident, one of four people infected by the H5N1 virus being treated in hospital, died on Tuesday after being admitted on June 23, the Lao Dong newspaper quoted hospital officials as saying. The Health Ministry said the bird flu had infected 60 people since it returned to Vietnam in December. On Wednesday, June 29, the World Health Organization (WHO) repeated its warning that the H5N1 virus could mutate into a form which could pass easily between people and cause a global pandemic. The virus, which arrived in Asia in late 2003, has also killed 12 Thais and four Cambodians. The Health Ministry has called on a campaign to raise public awareness and clean up the environment between now and December to combat the poultry virus, which seems to thrive best in the winter but still jumps to humans in the hot months.
Source: http://news.yahoo.com/news?tmpl=story&u=/nm/20050630/wl_nm/birdflu_vietnam_dc_2

22. *June 28, J. Craig Venter Institute* — **Major new policy study will explore risks, benefits of synthetic genomics.** On June 28, three organizations, the J. Craig Venter Institute (Venter Institute), the Center for Strategic & International Studies (CSIS), and the Massachusetts Institute of Technology (MIT), announced a new project to examine the societal implications of synthetic genomics, a new field involving the development of viruses and cells using designed and engineered DNA. The 15−month study will explore the risks and benefits of this emerging technology, as well as possible safeguards to prevent abuse, including bioterrorism. “The field of synthetic genomics has the potential for groundbreaking scientific advances, including the development of alternative energy sources, and the production of new vaccines and pharmaceuticals,” stated J. Craig Venter, Ph.D., founder and president of the Venter Institute. Funded by a $570,060 grant from the Alfred P. Sloan Foundation, the multi−organization effort will engage scientists and policymakers to better understand the potential risks and benefits associated with synthetic genomics. The study, expected to be completed by July 2006, will include a series of workshops analyzing technological and societal concerns. In addition, a meeting including policymakers, scientists, and the media will be conducted to discuss oversight, governance, and monitoring issues.
Source: http://www.venterinstitute.org/press/news/news_2005_06_28.php

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

23.

June 29, North Clermont Community Journal (OH) — **Expo will teach residents more about security.** Residents in Clermont County, OH, will soon have a chance to learn more about homeland security and how it affects them. A Homeland Security Expo will be held Wednesday, July 27, at the Clermont County Fairgrounds in Owensville. It will include demonstrations by a decontamination unit and explosive detection dogs, said Kathy Lehr, director of communications for Clermont County. Several other county and regional agencies will be featured as well. Lehr said it's not only important for the community to take measures to protect their residents, but it's also important residents know what's being done to protect them. At the expo, residents will have a chance to talk to, and interact with, emergency responders, she said. Ed Bridgeman, head of the criminal justice department at UC Clermont, will be giving a presentation about the current state of homeland security. "I'll be talking a little bit about terrorism and some of the threats, not just in America, but what we face in this region," he said. "It's critical for citizens to know who the terrorists are...so we can protect ourselves," he said.
Source: http://www.communitypress.com/GoshenTownshipOH/News.asp?pageType=StoryCurrent&StoryArchiveID=15204&StoryID=3345&Section=Main%20News&OnlineSection=Main%20News&SectionPubDate=Wednesday,%20June%2029,%202005&RefDate=6/29/2005

24. *June 29, Associated Press* — **Mock bioterrorism attack in Oklahoma scheduled for July.** Oklahoma state health officials are planning a drill for next month to test their preparedness in case of a bioterrorism attack. About 1,400 state and local medical personnel and numerous volunteers will stage the release of the pneumonic plague in Oklahoma City, Tulsa and Lawton on July 12th, 13th and 14th. State health Commissioner Doctor Mike Crutcher says the drill is an effort to test emergency response systems in case of a public health catastrophe. He says the goal is to demonstrate the Health Department's ability to request, receive and distribute emergency medical supplies in case of such a catastrophe.
Source: http://www.kotv.com/main/home/stories.asp?whichpage=1&id=858 03

25. *June 29, The Pasadina Citizen (TX)* — **Drill will test evacuation strategy.** In response to the state's new traffic management plan for mandatory evacuations during a hurricane, the Pasadena, TX, Office of Emergency Management will participate in a field drill Wednesday, July 6. According to Jennifer Shields Hawes, senior deputy coordinator for the Office of Emergency Management, the new traffic management plan has been designed to funnel Gulf Coast residents to northern cities and counties, in an attempt to relieve heavily stressed western and northwestern Texas cities. She said the state is working to develop shelters, and the mandatory evacuation routes will help divert residents to shelters and help evacuation points best utilize their resources. For Wednesday's drill, Hawes Shields said the emergency workers will familiarize themselves with the traffic signals and other traffic management equipment. Drills will also be held at the Emergency Operations Center, but will likely not be seen by the public.
Source: http://www.zwire.com/site/news.cfm?newsid=14778215&BRD=1574&PAG=461&dept_id=532238&rfi=6

26. *June 29, The Business Journal of Phoenix (AZ)* — **Arizona human and emergency services database goes online.** A statewide database designed to give the public instant access to health, human services and emergency response information made its debut in Arizona Wednesday, June 29. Governor Janet Napolitano unveiled Arizona 2−1−1 Online during her weekly press

briefing at the state Capitol, calling the Website a one−stop shop for Arizonans to learn about the latest emergency situations affecting the state, like the Cave Creek wildfires, in real time. The Web site, www.az211.gov, is Phase I of the multifaceted statewide system. In Phase II, call centers will be established to provide information and referrals to the public. In future phases, the database and call center operations will be enhanced. The governor did not set a timetable as to when the other phases will be implemented. In addition to accessing health and human services information, the public can view disaster response and homeland security information, including the locations of disaster relief organizations and services, obtain accurate updates regarding threats and disasters, and identify opportunities to volunteer in communities. The database contains more than 17,000 services throughout the system and is being updated daily, making it one of the most comprehensive emergency and health service information providers in the country.
Source: http://phoenix.bizjournals.com/phoenix/stories/2005/06/27/da ily33.html?jst=b_ln_hl

27. *June 29, U.S. Northern Command* — **Exercise to focus on nuclear terror scenario.** Joint Task Force Civil Support (JTF−CS) in Fort Monroe, VA, is planning its next exercise in August. Sudden Response 05 will be carried out as an internal command post exercise. The exercise is intended to train the JTF−CS staff to plan and execute Consequence Management operations in support of Federal Emergency Management Agency Region IV's response to a nuclear detonation. The scenario: a seafaring vessel transporting a 10−kiloton nuclear warhead makes its way into a port off the coast of Charleston, SC. Terrorists aboard the ship attempt to smuggle the warhead off the ship to detonate it. Some of the objectives for SR05 are to refine nuclear incident Concept of Operations, produce a CM Operation Order, refine command post set−up procedures and maintain situational awareness of multiple CM incidents.
Source: http://www.northcom.mil/index.cfm?fuseaction=news.showstory&storyid=C9BFBBAC−F3CA−BD2E−008C7B34AFE33114

[Return to top]

Information Technology and Telecommunications Sector

28. *July 01, zone−h* — **FreeBSD SA 05−15: TCP connection stall denial of service.** Two problems have been discovered in the FreeBSD TCP stack. First, when a TCP packets containing a timestamp is received, inadequate checking of sequence numbers is performed, allowing an attacker to artificially increase the internal "recent" timestamp for a connection. Second, a TCP packet with the SYN flag set is accepted for established connections, allowing an attacker to overwrite certain TCP options. Using either of the two problems an attacker with knowledge of the local and remote IP and port numbers associated with a connection can cause a denial of service situation by stalling the TCP connection. The stalled TCP connection my be closed after some time by the other host. In some cases it may be possible to defend against these attacks by blocking the attack packets using a firewall. Packets used to effect either of these attacks would have spoofed source IP addresses.
Source: http://www.zone−h.org/advisories/read/id=7757

29. *June 30, Security Focus* — **Apache HTTP request smuggling vulnerability.** Apache is prone to an HTTP request smuggling attack. A specially crafted request with a 'Transfer−Encoding: chunked' header and a 'Content−Length' can cause the server to forward a reassembled request

with the original 'Content−Length' header. Due to this, the malicious request may piggyback with the valid HTTP request. It is possible that this attack may result in cache poisoning, cross−site scripting, session hijacking and other attacks. This issue was originally described in BID 13873 (Multiple Vendor Multiple HTTP Request Smuggling Vulnerabilities). Due to the availability of more details and vendor confirmation, it is being assigned a new BID. The vendor has released Apache 2.1.6 to address this issue in the 2.1.x branch. A fix for the 2.0 branch is also available in the Apache SVN repository.
Source: http://www.securityfocus.com/bid/14106/solution

30. *June 29, Cisco Systems* — **RADIUS authentication bypass.** Remote Authentication Dial In User Service (RADIUS) authentication on a device that is running certain versions of Cisco Internetworking Operating System (IOS) and configured with a fallback method to none can be bypassed. Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected. Only the systems that are running certain versions of Cisco IOS are affected. Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected. Cisco has made software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.
Source: http://www.cisco.com/warp/public/707/cisco−sa−20050629−aaa.s html#impact

31. *June 29, FrSIRT* — **XML−RPC for PHP unspecified remote code execution vulnerability.** A vulnerability was identified in XML−RPC for PHP, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to an unspecified error which could be exploited via vulnerable scripts to execute arbitrary commands and compromise a vulnerable web server. No further details have been disclosed. The FrSIRT is not aware of any official supplied patch for this issue.
Source: http://www.frsirt.com/english/advisories/2005/0911

32. *June 29, Government Computer News* — **Federal government slated to transition to IPv6 by June 2008.** The federal government will transition to IP Version 6 (IPv6) by June 2008, said Karen Evans, the Office of Management and Budget's administrator of e−government and information technology. "Once the network backbones are ready, the applications and other elements will follow," she said Wednesday, June 29, while testifying before the House Government Reform Committee. Worldwide, IPv6 is already replacing IPv4 as the Internet address protocol of choice. Under IPv4, networked devices are assigned a 32−bit address. That limits the number of addresses to 4.3 billion. Once an unthinkably large number, it's not enough in a world where cell phones can connect to the Internet. Some organizations already resort to assigning a single address to an entire internal network and using a translator for individual devices. IPv6, however operates on a 128−bit address standard, which provides 340,282,366,920,938,463,463,374,607,431,768,211,456 possible addresses. OMB officials will issue guidance shortly for the transition to IPv6, Evans said. That memo will include a requirement that agencies become familiar with some of the pitfalls associated with the new standard.
Source: http://www.gcn.com/vol1_no1/daily−updates/36256−1.html

33. *June 29, US−CERT* — **Fake Microsoft Security Bulletin e−mail circulating.** US−CERT has received reports of an e−mail message circulating purporting to be a Microsoft Security

Bulletin. The e−mail directs the user to download and install an executable that is supposed to be a cumulative patch. Through the use of social engineering that attacker is hoping to trick the user into thinking they will be installing a cumulative patch when in fact they are installing a version of SDBot, a commonly used Trojan horse. This variant of SDBot is part of a family of backdoor Trojan horse programs commonly controlled remotely by an attacker via Internet Relay Chat (IRC). Some variants of SDBot may not be detected by anti−virus applications. In 2003, a similar email message masquerading as a Microsoft Security Bulletin was circulated via email. Users that clicked on the link in this email message were infected with the Swen mass−mailing worm. US−CERT recommends that users do not follow unsolicited web links received in email messages. Additionally, users should manually type in the URL when attempting to go to the Websites recommended in an email, install anti−virus software, and keep virus signature files up−to−date.
Source: http://www.us−cert.gov/current/current_activity.html#port5k

34. *June 20, Security Focus* — **Heimdal TelnetD remote buffer overflow vulnerability.** Heimdal telnetd is susceptible to a remote buffer overflow vulnerability. This issue is due to a failure of the application to properly bounds check user−supplied data prior to copying it to an insufficiently sized memory buffer. This vulnerability may be exploited by remote attackers to influence the proper flow of execution of the application, resulting in attacker−supplied machine code being executed in the context of the affected network service. The vendor has released upgraded versions of the affected software to address this issue.
Source: http://www.securityfocus.com/bid/13989/solution

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT reports VERITAS has released security advisories disclosing vulnerabilities that affect multiple versions of Backup Exec for Windows and Netware Servers. Several components of Backup Exec are affected, including the Remote Agent, Server, NetBackup, Web Administration Console, and Admin Plus Pack Option. For more information, please see: http://www.us−cert.gov/current/current_activity.html

The impact of the vulnerabilities ranges from Denial of Service (DoS) conditions to remote execution of arbitrary code. VERITAS has released patches to eliminate all of the reported issues. It is strongly recommended that administrators apply the patches immediately, as historically, vulnerabilities affecting Backup Exec have been targeted by attackers in a widespread fashion:
http://support.veritas.com/menu_ddProduct_BEWNT_view_ALERT.h tm

Updated Port Status: Reports of increased activity on port 6101 have continued. Activity targeting TCP port 10000 has significantly increased since the release of the

Metasploit Framework module. Administrators are strongly urged to apply the hotfixes as soon as possible. Strict filtering of TCP port 10000 and 6101 is also highly recommended. For specific hotfixes and udpates please review the following URLs:
http://seer.support.veritas.com/docs/276604.htm
http://www.metasploit.org/projects/Framework/modules/exploits/backupexec_agent.pm

Current Port Attacks

Top 10 Target Ports	135 (epmap), 445 (microsoft−ds), 137 (netbios−ns), 1026 (−−−), 139 (netbios−ssn), 25 (smtp), 1434 (ms−sql−m), 1027 (icq), 1433 (ms−sql−s), 80 (www) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

35. *June 30, Associated Press* — **Arizona wildfire grows.** A lightning−sparked wildfire in central Arizona has grown to nearly 173,000 acres and residents in at least three communities surrounded by pine forest fear they could be in harm's way. The blaze was burning about 20 miles southwest of the mountain communities of Pine and Strawberry −− 12 miles from the point when evacuations there may be necessary. By Wednesday, June 29, the fire was also less than six miles west of Black Canyon City, a community of about 4,500 residents north of Phoenix, but wasn't considered an imminent threat to structures there. On the eastern flank, firefighters worked to stop flames from jumping over the Verde River. Authorities were concerned that if it crossed the river, it could push into a canyon and race into Pine and Strawberry, which are just three miles apart and have fewer than 5,000 year−round residents. The National Interagency Fire Center said Wednesday that 22 active large fires had burned across more than 905,000 acres in Alaska, Arizona, Colorado, Nevada, New Mexico, and Utah. In Nevada, the total fire zone covers approximately 500,000 acres.
Source: http://www.thestate.com/mld/thestate/news/nation/12017576.ht m

[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer